The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

12/10/2013

SUBJECT:

Cumulative Security Update for Internet Explorer (MS13-097)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Internet Explorer. The details of these vulnerabilities are as follows:

- Two elevation of privilege vulnerabilities, which exist during the validation of local file installation and during secure creation of registry keys.
- Five memory corruption vulnerabilities, which occur due to the way Internet Explorer improperly accesses objects in memory. These vulnerabilities could be exploited if a user visits a web page that is specifically crafted to take advantage of the vulnerabilities.

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Microsoft:

https://support.microsoft.com/kb/2898785

https://technet.microsoft.com/en-us/security/bulletin/ms13-097

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5045

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5046

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5047

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5048

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5049

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5051

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5052